PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-131452
(43)Date of publication of application : 19.05.1995

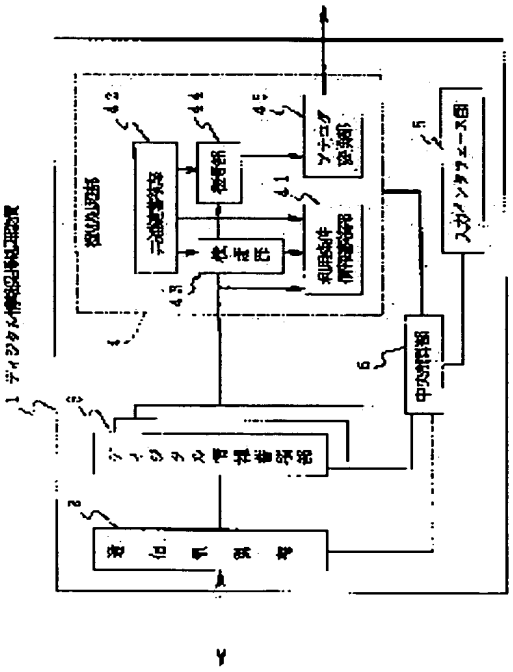
(51)Int.Cl. H04L 9/06
H04L 9/14
G06F 9/06
G09C 1/00

(21)Application number : 05-275388
(22)Date of filing : 04.11.1993

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : YAMANAKA KIYOSHI
KOYAIZU IKURO
TANABE KATSUHIRO

(54) DIGITAL INFORMATION PROTECTION METHOD AND ITS PROCESSOR

(57)Abstract:
PURPOSE: To provide the digital information protection method and its processor which protect information from the wrong action like wrong copy or alteration of data after reception.
CONSTITUTION: Digital information including the information main body enciphered by a common key and use condition information is received through a communication control part 2 and is stored in a digital information storage part, and use condition information is stored in a use condition information storage part 41 in a security processing part 4. The common key is preliminarily stored in a common key storage part 32, and alteration verification of digital information inputted from the digital information storage part 3 to the security processing part 4 is performed by a verification part 43. The common key is used to decipher the digital information inputted to the security processing part 4 by a deciphering part 44 based an the verification result. Further, deciphered digital information is converted to analog information by an analog conversion part 45 and is outputted. Thus, the rights and profits of a writer and an information presenter are protected.



LEGAL STATUS

[Date of request for examination]	19.11.1999
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3276021
[Date of registration]	08.02.2002
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平7－131452

(43)公開日　平成７年(1995)５月19日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/06				
	9/14				
Ｇ０６Ｆ	9/06	５５０　Ｚ	9367－5B		
Ｇ０９Ｃ	1/00		9364－5L		
				Ｈ０４Ｌ　9/ 02　Ｚ	

審査請求　未請求　請求項の数２　ＯＬ　（全 9 頁）

(21)出願番号　特願平5－275388

(22)出願日　平成５年(1993)11月４日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　山中　喜義
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　小柳津　育郎
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　田辺　克弘
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　吉田　精孝

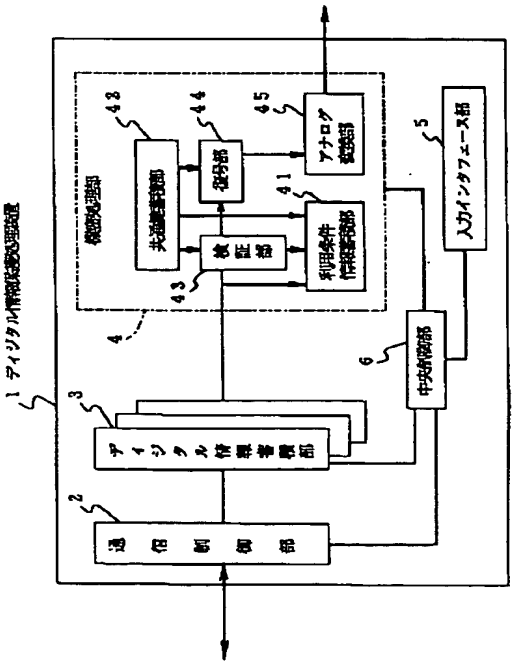
(54)【発明の名称】　ディジタル情報保護方法及びその処理装置

(57)【要約】

【目的】　受信後のデータの不正コピー、改ざん等の不正行為に対して情報を保護するディジタル情報保護方法及びその処理装置を提供すること。

【構成】　通信制御部２を介して、共通鍵で暗号化された情報本体及び利用条件情報を含むディジタル情報を受信してディジタル情報蓄積部に蓄積すると共に、利用条件情を機密処理部４内の利用条件情報蓄積部４１に蓄積する。また、共通鍵は共通鍵蓄積部３２に予め格納されており、ディジタル情報蓄積部３から機密処理部４に入力されたディジタル情報の改ざん検証を検証部４３によって行う。この検証結果に基づいて、復号部４４により、機密処理部４に入力されたディジタル情報を共通鍵を用いて復号する。さらに、復号されたディジタル情報をアナログ変換部４５によってアナログ情報に変換して出力する。

【効果】　著作権者並びに情報提供業者の権利及び利益を保護できる。



1

【特許請求の範囲】

【請求項1】　共通鍵蓄積部に蓄積される共通鍵で暗号化された通信毎に異なる通信用暗号鍵と、該通信用暗号鍵で暗号化された情報識別番号と、情報本体と、利用条件情報及び第1の認証子とで構成されるディジタル情報を通信回線経由により受信して、

該ディジタル情報をディジタル情報蓄積部に蓄積すると同時に、前記情報識別番号及び利用条件情報を機密処理部に転送し、

該機密処理部において前記情報識別番号及び利用条件情報から第2の認証子を計算すると共に、

該第2の認証子と前記情報識別番号及び利用条件情報を利用条件情報蓄積部に蓄積し、

情報利用時には、利用したいディジタル情報を前記ディジタル情報蓄積部より前記機密処理部に転送し、

前記機密処理部において、前記共通鍵蓄積部に蓄積される共通鍵を用い、前記ディジタル情報の内容の改ざん検証、並びに前記第1及び第2の認証子に基づいて前記利用条件蓄積部に格納されている利用条件情報内容の改ざん検証を行うと共に、利用回数、利用期間等の利用条件の適合検証を行い、

前記全ての検証を満足した場合にのみ、前記情報本体を復号部によって復号すると共に、アナログ変換部により人間の感覚で感知できる形態に変換した情報を出力した後、

前記利用条件情報蓄積部に蓄積されている情報内容及び認証子を更新または利用条件を満たさなくなった場合は削除することを特徴とするディジタル情報保護方法。

【請求項2】　共通鍵で暗号化された情報本体及び利用条件情報を含むディジタル情報を通信回線を介して受信する通信制御部と、

該通信制御部により受信したディジタル情報を蓄積するディジタル情報蓄積部と、

機密処理部とを備え、

該機密処理部は、ディジタル情報の利用条件情報を蓄積する利用条件情報蓄積部と、

前記共通鍵を蓄積する共通鍵蓄積部と、

前記共通鍵蓄積部に蓄積されている共通鍵を用いて、前記ディジタル情報蓄積部から入力したディジタル情報の改ざん検証を行う検証部と、

該検証部の検証結果に基づいて、前記共通鍵蓄積部に蓄積されている共通鍵を用いて、前記ディジタル情報蓄積部から入力したディジタル情報を復号する復号部と、

該復号されたディジタル情報をアナログ情報に変換して出力するアナログ変換部とから構成されることを特徴とするディジタル情報処理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、音楽・映像・絵画・コンピュータグラフィックス等の著作物情報をＩＳＤＮ等

2

の通信回線を介してディジタル情報として受信した後、アナログ変換して利用する際、受信後の情報の改ざん、不正コピー、不正使用等を防止して著作権者・情報提供者の権利を保護するディジタル情報保護方法及びその処理装置に関するものである。

【0002】

【従来の技術】近年、音声・静止画・動画等のディジタル情報圧縮技術（例えば、MPEG, JPEG方式等）及びＩＳＤＮを代表とするディジタル通信技術の発達により、音楽・映像・絵画・コンピュータグラッフィクス等の著作物をディジタル情報に変換・圧縮符号化して通信回線を利用して送信することが実現可能となってきた。映像等のディジタル情報に比べデータ量の少ないコンピュータソフトウェアでは、既にパソコン通信等を利用した配送サービスを実施している例がある。

【0003】通信回線を利用してディジタル情報を購入する場合、料金を事前に支払ってから利用する方法と、先にディジタル情報を受信してから利用度に応じて事後に支払う方法がある。

【0004】そのうち、料金を事前に支払う方法でも、契約内容により、取得した情報を利用回数・利用期間等の制限条件付きで利用する方法と、制限条件なしに利用できる方法が考えられている。

【0005】

【発明が解決しようとする課題】前述したように、料金を事前に支払ってから情報を取得して利用する場合、取得した情報をディジタル形式で不正に複製して他の装置で利用したり、利用回数・利用期間等の制限条件を書換えて制限以上に使用したりする不正行為により、著作権者・情報提供業者の権利、利益を侵害する恐れが生じる。

【0006】従来のパソコン通信利用によるコンピュータソフトウェア配送では、情報提供元となるセンタと接続する時に、ユーザＩＤ、パスワードによる相手確認を行う程度で受信後のデータの不正コピー、改ざん等の不正行為に対して防止対策が施されていなかった。

【0007】本発明の目的は上記の問題点に鑑み、受信後のデータの不正コピー、改ざん等の不正行為に対して情報を保護するディジタル情報保護方法及びその処理装置を提供することにある。

【0008】

【課題を解決するための手段】本発明は上記の目的を達成するために、請求項1では、共通鍵蓄積部に蓄積される共通鍵で暗号化された通信毎に異なる通信用暗号鍵と、該通信用暗号鍵で暗号化された情報識別番号と、情報本体と、利用条件情報及び第1の認証子とで構成されるディジタル情報を通信回線経由により受信して、該ディジタル情報をディジタル情報蓄積部に蓄積すると同時に、前記情報識別番号及び利用条件情報を機密処理部に転送し、該機密処理部において前記情報識別番号及び利

用条件情報から第２の認証子を計算すると共に、該第２の認証子と前記情報識別番号及び利用条件情報を利用条件情報蓄積部に蓄積し、情報利用時には、利用したいディジタル情報を前記ディジタル情報蓄積部より前記機密処理部に転送し、前記機密処理部において、前記共通鍵蓄積部に蓄積される共通鍵を用い、前記ディジタル情報の内容の改ざん検証、並びに前記第１及び第２の認証子に基づいて前記利用条件蓄積部に格納されている利用条件情報内容の改ざん検証を行うと共に、利用回数、利用期間等の利用条件の適合検証を行い、前記全ての検証を満足した場合にのみ、前記情報本体を復号部によって復号すると共に、アナログ変換部により人間の感覚で感知できる形態に変換した情報を出力した後、前記利用条件情報蓄積部に蓄積されている情報内容及び認証子を更新または利用条件を満たさなくなった場合は削除するディジタル情報保護方法を提案する。

【０００９】また、請求項２では、共通鍵で暗号化された情報本体及び利用条件情報を含むディジタル情報を通信回線を介して受信する通信制御部と、該通信制御部により受信したディジタル情報を蓄積するディジタル情報蓄積部と、機密処理部とを備え、該機密処理部は、ディジタル情報の利用条件情報を蓄積する利用条件情報蓄積部と、前記共通鍵を蓄積する共通鍵蓄積部と、前記共通鍵蓄積部に蓄積されている共通鍵を用いて、前記ディジタル情報蓄積部から入力したディジタル情報の改ざん検証を行う検証部と、該検証部の検証結果に基づいて、前記共通鍵蓄積部に蓄積されている共通鍵を用いて、前記ディジタル情報蓄積部から入力したディジタル情報を復号する復号部と、該復号されたディジタル情報をアナログ情報に変換して出力するアナログ変換部とから構成されるディジタル情報処理装置を提案する。

【００１０】

【作用】本発明の請求項１によれば、ディジタル情報は、共通鍵蓄積部に蓄積される共通鍵で暗号化された通信毎に異なる通信用暗号鍵と、該通信用暗号鍵で暗号化された情報識別番号と、情報本体と、利用条件情報及び第１の認証子とで構成される。該ディジタル情報が通信回線経由によって受信されると、該ディジタル情報はディジタル情報蓄積部に蓄積され、これと同時に前記情報識別番号及び利用条件情報が機密処理部に転送される。この後、前記機密情報処理部において前記情報識別番号及び利用条件情報から第２の認証子が計算されると共に、該第２の認証子並びに前記情報識別番号及び利用条件情報が利用条件情報蓄積部に蓄積される。また、情報利用時には、利用したいディジタル情報が前記ディジタル情報蓄積部より前記機密処理部に転送され、前記機密処理部において、前記共通鍵を用いて前記ディジタル情報の内容の改ざん検証、並びに前記第１及び第２の認証子に基づいて前記利用条件蓄積部に格納されている利用条件情報内容の改ざん検証が行われると共に、利用回数、利用期間等の利用条件の適合検証が行われ、前記全ての検証を満足した場合にのみ、前記情報本体が復号部によって復号されると共に、アナログ変換部によって人間の感覚で感知できる形態、例えばＣＲＴモニタに表示された画像或いは音声等の形態に変換されて情報出力される。この後、前記利用条件情報蓄積部に蓄積されている情報内容及び認証子が更新されるか、または、利用条件を満たさなくなった場合に削除される。

【００１１】また、請求項２によれば、通信回線を介して通信制御部により、共通鍵で暗号化された情報本体及び利用条件情報を含むディジタル情報が受信され、該通信制御部により受信されたディジタル情報はディジタル情報蓄積部に蓄積される。さらに、前記利用条件情報は機密処理部内の利用条件情報蓄積部に蓄積される。また、前記共通鍵は共通鍵蓄積部に蓄積され、検証部によって前記ディジタル情報蓄積部から機密処理部に入力されたディジタル情報の改ざん検証が行われ、該検証部の検証結果に基づいて、復号部により、前記共通鍵蓄積部に蓄積されている共通鍵を用いて、前記ディジタル情報蓄積部から機密処理部に入力されたディジタル情報が復号される。さらに、該復号されたディジタル情報がアナログ変換部によってアナログ情報に変換されて出力される。これにより、前記共通鍵で暗号化された情報本体及び利用条件情報を含むディジタル情報は、利用時に機密処理部内で該ディジタル情報が検証されて適合した場合にのみ、前記情報本体が復号されると共にアナログ変換され利用可能状態とされる。

【００１２】

【実施例】以下、図面に基づいて本発明の一実施例を説明する。図１は、本発明の一実施例のディジタル情報保護処理装置の構成を示す図である。図において、１はディジタル情報保護処理装置で、通信回線を介してディジタル情報を受信する通信制御部２、通信制御部２によって受信したディジタル情報を蓄積するディジタル情報蓄積部３、機密処理部４、及びキーボード等からなる入力インタフェース部５に接続され、各部の動作制御を行う中央制御部６から構成されている。

【００１３】機密処理部４は、ディジタル情報保護処理装置１を操作する操作者から隠蔽されており、前記ディジタル情報内に含まれる利用回数・利用期間等が記述された利用条件情報を蓄積する利用条件情報蓄積部４１、各装置固有の共通鍵を蓄積する共通鍵蓄積部４２、ディジタル情報の改ざん検証、利用条件情報内容の検証等を行う検証部４３、ディジタル情報及び通信用暗号鍵等を復号する復号部４４、復号されたディジタル情報をアナログ情報に変換するアナログ変換部４５から構成されている。

【００１４】次に、本実施例の動作を説明する。まず、ディジタル情報保護処理装置（以下、情報処理装置と称する）１によってディジタル情報を受信し、これを蓄積

5

するまでの動作を図２乃至図５に基づいて説明する。操作者は情報処理装置１を用いて、音楽・映像・絵画・コンピュータグラフィックス等のディジタル情報を提供する情報センタに通信回線を介してアクセスし（Ｓ１）、所望のディジタル情報を検索する（Ｓ２）。

【００１５】通信制御部１を介して受信したディジタル情報は、ディジタル情報蓄積部３に蓄積される（Ｓ３）。このとき、ディジタル情報蓄積部３には、その蓄積容量に応じて複数のディジタル情報が同時に蓄積される。

【００１６】図３に本実施例において処理対象とするディジタル情報の形式を示す。図において、Ｋａは共通鍵で、各情報処理装置で固有の鍵であり、予め共通鍵蓄積部４２に蓄積されている。Ｋｓは通信用暗号鍵で、ディジタル情報本体等を暗号化するためのものであり、各通信毎に可変である。Ｋａ（Ｋｓ）は、通信用暗号鍵Ｋｓを共通鍵Ｋａで暗号化した値である。また、Ｋｓ（情報識別番号）、Ｋｓ（情報本体）、Ｋｓ（利用条件情報）は、情報識別番号、情報本体、及び利用条件情報のそれぞれを通信用暗号鍵Ｋｓによって暗号化した情報であり、Ｎａは認証子である。

【００１７】共通鍵Ｋａの値は、情報提供業者と契約して本ディジタル情報保護処理装置１を入手した時点で、共通鍵蓄積部４２に既に書き込まれており、情報提供業者は既知であるが、機密処理部４内に隠蔽されているため、本装置１の利用者からは未知の値となっている。

【００１８】情報識別番号は、受信した各ディジタル情報を一意に識別する番号であり、情報提供元となる情報センタで付与される。情報本体は音楽・映像・絵画・コンピュータグラフィックス等を圧縮符号化したディジタル情報の実態部分である。利用条件情報は、情報提供業者との契約時にディジタル情報購入金額に応じて設定した利用に関する制限条件を記述した情報である。

【００１９】図４は、前述した利用条件情報の内容の一例を示す図である。図４に示す例では、利用・試用できる回数、及び利用・試用できる期間を開始年月日と停止年月日で規定している。ここで、試用とは情報内容の一部のみを復号及びアナログ変換できることを言う。例えば、音楽著作物の場合、試用においては全曲を聴くことができず、冒頭部分のみ再生して聞くことができる。利用条件情報は、図４に示す内容の一部だけ記載してもよい。例えば、試用のみ可能で利用は不可とする場合の利用条件情報は、

利用回数＝０
試用回数＝ｎ（ｎ＞０）
試用開始年月日＝”ｙｙ1 mm1 ｄｄ1 ”
試用停止年月日＝“ｙｙ2 mm2 ｄｄ2 ”

となり、利用開始年月日、利用停止年月日は省略される。

【００２０】また、利用回数または利用期間に制限がない契約の場合は、例えば、以下の通り記述される。

利用回数＝－１
利用停止年月日＝”０００００”

図３に示す認証子Ｎａは、受信されたディジタル情報の内容の改ざんを検出するためのチェックデータであり、通信用暗号鍵Ｋｓで暗号化された情報識別番号、情報本体、利用条件情報に対して例えばＭＡＣ（詳細は、ＩＳ０９７９７参照）等のデータ改ざん検出用認証子作成方法により情報センタで計算して付与される。このとき、認証子Ｎａの作成用鍵として共通鍵Ｋａを用いているので、本装置１の操作者が不正行為によって改ざんを検出されない様に変更することは困難となる。

【００２１】前述したディジタル情報がディジタル情報蓄積部３に蓄積されると同時に、通信用暗号鍵Ｋｓで暗号化された情報識別番号と利用条件情報は機密処理部４に転送され（Ｓ４）、前記ディジタル情報内の認証子Ｎａと同様の方式で情報識別番号及び利用条件情報に対して計算した認証子Ｎａ’が算出され（Ｓ５）、該認証子Ｎａ’は利用条件情報蓄積部４１に書き込まれる（Ｓ６）。

【００２２】図５に利用条件情報蓄積部４１に格納される情報形式を示す。図に示すように、利用条件情報蓄積部４１には、通信用暗号鍵Ｋｓで暗号化された情報識別番号と利用条件情報、及び認証子Ｎａ’が格納される。

【００２３】次に、前述の手順でディジタル情報を受信、蓄積した後の利用手順を図６のフローチャートに基づいて説明する。情報処理装置１の操作者は、まず、ディジタル情報蓄積部３に蓄積された複数のディジタル情報のうち、利用したい（見たい、聴きたい）ディジタル情報を選択した後（ＳＰ１）、該情報を利用するのか或いは試用するのかの何れかを指定する（ＳＰ２）。これにより選択されたディジタル情報は、ディジタル情報蓄積部３から機密処理部４に転送される（ＳＰ３）。

【００２４】機密処理部４に転送されたディジタル情報は、検証部４３によってデータ内容の改ざんが検証される。ここで行われる第１の検証は、受信されたディジタル情報内容の改ざん検出である。即ち、通信用暗号鍵Ｋｓで暗号化された情報識別番号及び情報本体並びに利用条件情報に対して、共通鍵蓄積部４２内の共通鍵Ｋａを用いて認証子データ（以下、ＭＡＣ１’と称する）を作成し、該ＭＡＣ１’と、受信されたディジタル情報内に記載された認証子Ｎａ（以下、ＭＡＣ１と称する）とを照合する（ＳＰ４）。この照合の結果、ＭＡＣ１≠ＭＡＣ１’のときは、受信されたディジタル情報は改ざんされたと判定し、利用不可として操作者に通知し以後の処理を中断する（ＳＰ５）。

【００２５】また、第１の検証の結果、ＭＡＣ１＝ＭＡＣ１’の場合、第２の検証が行われる（ＳＰ６）。第２の検証は、利用条件情報内容の改ざん検出である。即ち、受信時に利用条件情報蓄積部４１に転送・蓄積され

た複数の情報識別番号・利用条件情報・認証子のセットのうち、前記選択されたディジタル情報と同一の情報識別番号を有するセットを検索し、共通鍵蓄積部４２内の共通鍵Ｋａを用いて認証子データ（以下、ＭＡＣ２’と称する）を作成し、該ＭＡＣ２’と、利用条件情報蓄積部３２に格納されている認証子Ｎａ’（以下、ＭＡＣ２と称する）とを照合する（ＳＰ６）。この照合の結果、ＭＡＣ２≠ＭＡＣ２’のときは、利用条件情報が改ざんされたものと判定し、利用不可として操作者に通知する（ＳＰ５）。

【００２６】また、前記検索の結果、利用したいディジタル情報と同一の情報識別番号を有する利用条件情報が、利用条件情報蓄積部４１に存在しなかった場合には、他人からの不正コピーによる使用、或いは利用回数・利用期間超過等の理由により利用条件を満足しなかったものと判定し、利用不可として操作者に通知し以降の処理を中断する（ＳＰ５）。

【００２７】前述したＳＰ４，ＳＰ６の検証に適合した場合、即ちＭＡＣ１＝ＭＡＣ１’かつＭＡＣ２＝ＭＡＣ２’であるときには、該当ディジタル情報内の情報識別番号と同一の情報識別番号を有する利用条件情報を利用条件情報蓄積部４１から抽出し、共通鍵蓄積部４２に格納されている共通鍵Ｋａを用いて復号した通信用暗号鍵Ｋｓにより前記抽出した利用条件情報を復号して、利用条件内容を検証する（ＳＰ７）。

【００２８】まず情報を利用する場合は、図４に示す利用条件情報で、以下の条件を満足するかを検証する。「利用回数　０（－１か正の整数）」かつ「利用開始年月日≦現在年月日≦利用停止年月日　または　利用停止年月日＝“０００００００“（期間制限なし）」。

【００２９】次に情報を試用する場合は、図４に示す利用条件情報で、以下の条件を満足するかを検証する。「試用回数　０（－１か正の整数）」かつ「試用開始年月日≦現在年月日≦試用停止年月日　または　試用停止年月日＝“０００００００“（期間制限なし）」。

【００３０】上記条件を満足する場合、復号部４４により図３に示すディジタル情報内の情報本体を通信用暗号鍵Ｋｓで復号する（ＳＰ８）。この後、アナログ変換部３５により、人間の感覚で感知できるアナログ情報の形態、即ち音楽を耳で聴ける、映像を目で見られる等の形態に変換し（ＳＰ９）、操作者に情報（試用の場合は、情報の一部）を提供する。

【００３１】ここで、通信用暗号鍵Ｋｓは共通鍵Ｋａによって暗号化されているため、本情報処理装置１を用いて正規に受信したディジタル情報のみが正しく復号され、他の情報処理装置で受信したディジタル情報は正しく復号されない。

【００３２】最後に、該利用或いは試用したディジタル情報に対応する利用条件情報蓄積部４１内の利用条件情報を更新する（ＳＰ１０）。即ち、情報利用または情報

試用の場合に応じて、それぞれ利用回数、試用回数を１減算した後、図５に示す情報識別番号と変更後の利用条件情報に対して改めて認証子Ｎａ’を計算して書き換える。また、利用・試用回数無制限（利用・試用回数＝－１）の場合は、変更操作は不要である。この時点で、利用条件を満たさなくなった場合、具体的には、「利用回数＝０　または　現在年月日≧利用停止年月日」かつ「試用回数＝０　または現在年月日≧試用停止年月日」の場合、該当する情報識別番号、利用条件情報及び認証子Ｎａ’を利用条件情報蓄積部４１から削除する。

【００３３】以上に示した手順を繰り返すことにより、複数のディジタル情報の受信から利用まで可能となる。

【００３４】これにより、受信したディジタル情報をそのままコピーして他の装置等で復号、アナログ変換しても、本来の意図する情報は復元されず、不正コピーを防止できる。また、受信したディジタル情報及び利用条件情報に認証子を付与しているので、受信情報および利用条件情報を改ざんした場合、共通鍵Ｋａを知らない限り、利用時の検証で改ざん検出がなされ、情報を復号、アナログ変換することができず改ざん防止が可能となる。

【００３５】尚、本実施例の情報処理装置１は、コンピュータソフトウェアの様なディジタル形式のままで利用する必要のある著作物の配送後の著作物保護方法にも一部（プログラム実行時の展開メモリ上での実行ファイル盗用防止を除く）応用可能である。

【００３６】また、本実施例では、認証子作成、情報の暗号化をすべて共通鍵暗号方式で実施しているが、本情報処理装置１が大量に流通する場合、復号速度に余裕のある認証、通信暗号鍵の復号等には、鍵管理・配送の容易な公開鍵暗号方式を用いて実施しても同等の効果があることは言うまでもないことである。

【００３７】

【発明の効果】以上説明したように本発明の請求項１記載のディジタル情報保護方法によれば、認証子及び利用条件情報付きのディジタル情報を共通鍵暗号方式を用いた暗号通信により受信し、利用時に機密処理部内で認証子及び利用条件情報を検証して適合した場合にのみ、情報本体を復号・アナログ変換した後、利用条件情報を認証子と共に書き換えるので、前記受信したディジタル情報をそのままコピーしても、共通鍵を知らない限り他の装置等を用いて情報を復号・アナログ変換した結果では意図する情報は復元されないため、不正コピーを防止することができる。また、受信情報および利用条件情報に認証子を付与することにより、受信情報及び利用条件情報を改ざんした場合においても、共通鍵を知らない限り、利用時の検証により改ざんを検出し、情報本体を復号・アナログ変換しないので、改ざんによる不正使用も防止することができる。また、ディジタル情報蓄積部に蓄積された受信情報をそのままコピーして保存してお

9

き、利用時に再度同一のディジタル情報保護処理装置のディジタル情報蓄積部に戻してから情報本体を復号・アナログ変換して利用することができるため、ディジタル情報蓄積部の蓄積容量制限以上に受信しても外部記憶装置に保存しておき、必要に応じて利用することができる。さらにこれにより、ディジタル情報蓄積部のファイルの人為的でない物理的破壊等に備えてのバックアップコピーとしても利用できるという大きな効果が得られる。

【００３８】また、請求項２記載のディジタル情報保護処理装置によれば、共通鍵で暗号化された情報本体及び利用条件情報を含むディジタル情報は、利用時に機密処理部内で該ディジタル情報が検証されて適合した場合にのみ、前記情報本体が復号されると共にアナログ変換され、利用可能状態とされるので、前記受信したディジタル情報をそのままコピーしても、共通鍵が蓄積されていない他の装置等を用いて情報を復号・アナログ変換した結果では意図する情報を復元することができない。従って、該ディジタル情報保護処理装置を使用することにより、不正コピーを防止することができる。さらに、共通鍵を知らない限り、受信情報及び利用条件情報を改ざんした場合においても、利用時の検証により改ざんが検出され、情報本体は復号・アナログ変換されないので、改ざんによる不正使用も防止することができる。また、ディジタル情報蓄積部に蓄積された受信情報をそのまま外部記憶装置にコピーして保存しておき、利用時に再度同一のディジタル情報保護処理装置のディジタル情報蓄積

10

部に戻してから情報本体を復号・アナログ変換して利用することもできるため、ディジタル情報蓄積部の蓄積容量制限以上に受信しても外部記憶装置に保存しておき、必要に応じて利用することができる。さらにこれにより、ディジタル情報蓄積部のファイルの人為的でない物理的破壊等に備えてのバックアップコピーとしても利用できるという非常に優れた効果を奏するものである。

【図面の簡単な説明】

【図１】本発明の一実施例のディジタル情報保護処理装置を示す構成図

【図２】一実施例における情報受信及び蓄積動作を説明するフローチャート

【図３】一実施例において処理対象とするディジタル情報の形式を示す図

【図４】一実施例におけるディジタル情報内の利用条件情報の内容例を示す図

【図５】一実施例における利用条件情報蓄積部の蓄積情報内容を示す図

【図６】一実施例における情報利用時の動作を説明するフローチャート

【符号の説明】

１…ディジタル情報保護処理装置、２…通信制御部、３…ディジタル情報蓄積部、４…機密処理部、４１…利用条件情報蓄積部、４２…共通鍵蓄積部、４３…検証部、４４…復号部、４５…アナログ変換部、５…入力インタフェース部、６…中央制御部。

【図３】

Ka(Ks)	Ks(情報識別番号)	Ks(情報本体)	Ks(利用条件情報)	認証子Ｎａ

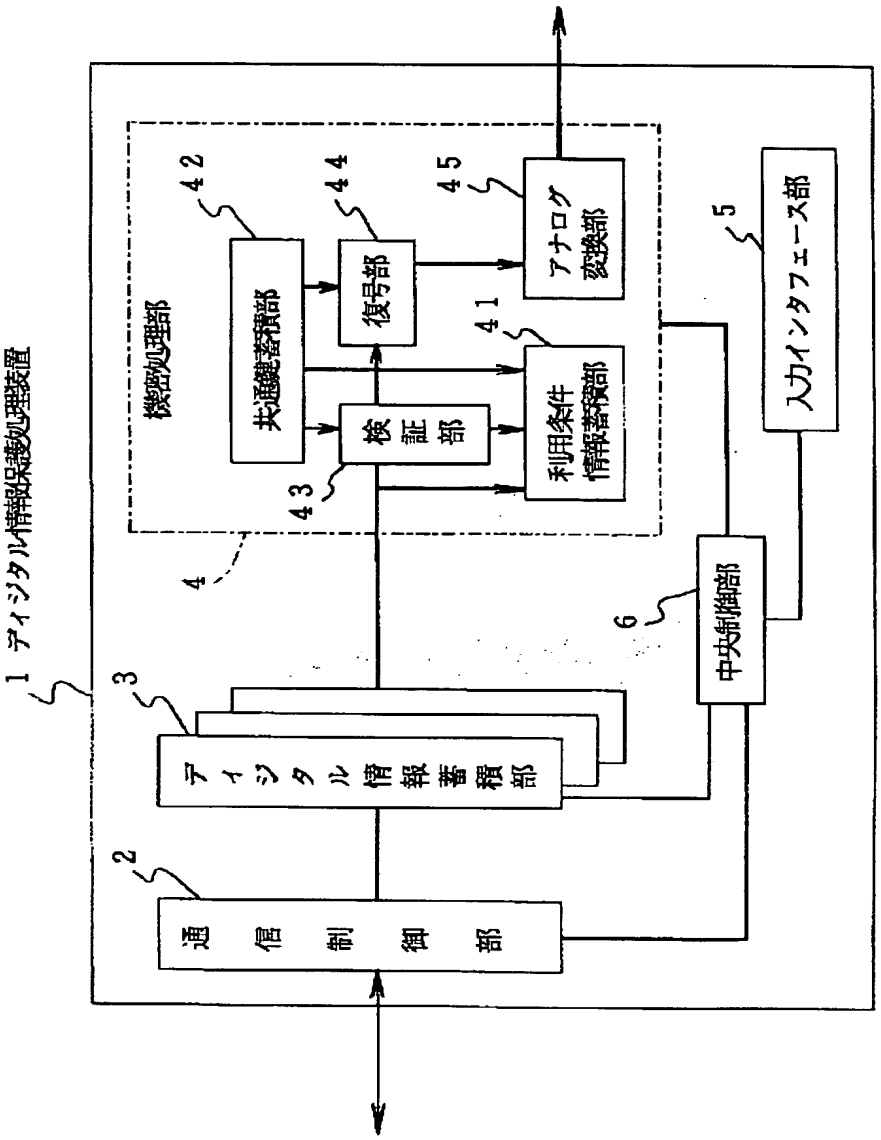
【図４】

利用回数	試用回数	利用開始年月日	利用停止年月日	試用開始年月日	試用停止年月日

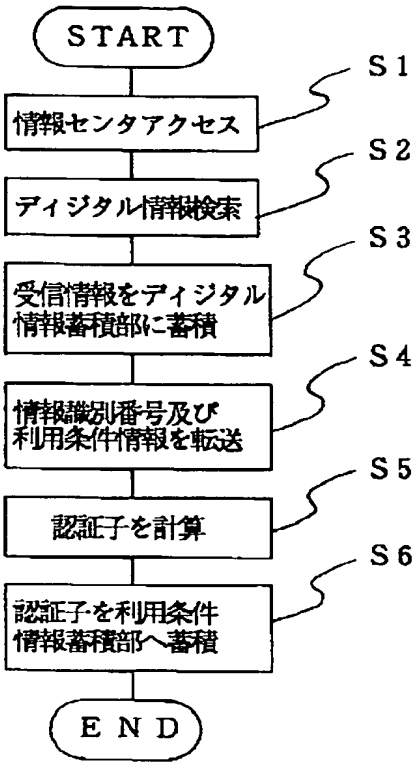
【図５】

Ks(情報識別番号)	Ks(利用条件情報)	認証子Ｎａ'

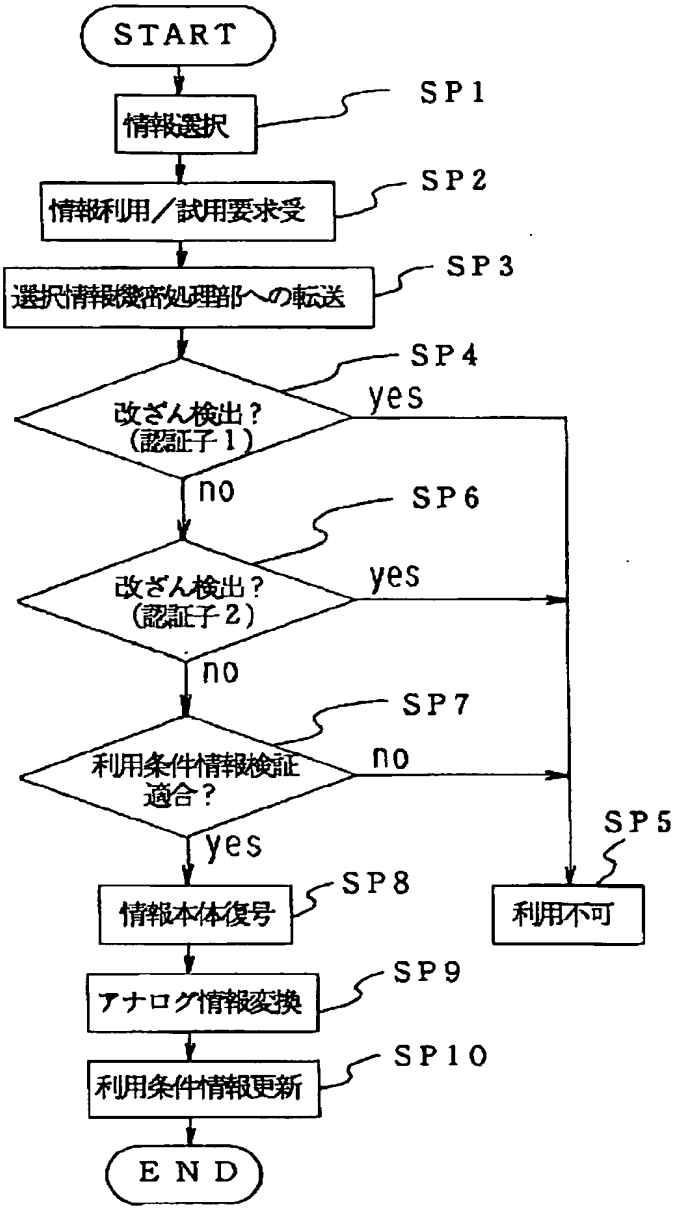
【図1】


1 ディジタル情報保護処理装置
2
通信制御部
3
ディジタル情報蓄積部
4
機密処理部
41
利用条件情報蓄積部
42
共通鍵蓄積部
43
検証部
44
復号部
45
アナログ変換部
5
入力インタフェース部
6
中央制御部

【図2】


START
S1
情報センタアクセス
S2
ディジタル情報検索
S3
受信情報をディジタル情報蓄積部に蓄積
S4
情報識別番号及び利用条件情報を転送
S5
認証子を計算
S6
認証子を利用条件情報蓄積部へ蓄積
END

【図6】


START
情報選択
SP1
情報利用／試用要求受
SP2
選択情報機密処理部への転送
SP3
改ざん検出？
(認証子1)
SP4
yes
no
改ざん検出？
(認証子2)
SP6
yes
no
利用条件情報検証
適合？
SP7
no
yes
利用不可
SP5
情報本体復号
SP8
アナログ情報変換
SP9
利用条件情報更新
SP10
END

This Page Blank (uspto)